

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF SOUTH CAROLINA
COLUMBIA DIVISION

In The Matter of the Seizure of Funds, Monies,
and Other Things of Value not to Exceed
80,736.10 USDT (TetherUS) and 7.2799 BTC
(Bitcoin) Stored in or Accessible at Binance
Associated with the Following “**Target
Cryptocurrency Account:**”

HAIDER ALI

Case No. 3:24-cr-00818

Affidavit in Support of An Application for a Seizure Warrant

I, Clinton Walker, being first duly sworn, hereby depose and state as follows:

Introduction and Background

I am a Special Agent of the South Carolina Law Enforcement Division (SLED) and Task Force Officer of the United States Secret Service South Carolina Cyber Fraud Task Force (USSS SC CFTF) and have been so employed since January 2023. As a Special Agent of SLED, I received extensive training at the South Carolina Criminal Justice Academy. This training covered aspects of criminal investigation and law enforcement. I have participated in numerous investigations of violations of criminal law, including matters involving fraud and white-collar crime. I have attended numerous training courses involving financial related crimes and crimes involving cryptocurrency.

This affidavit does not purport to set forth all my knowledge or investigation concerning this case. The statements contained in this affidavit are based on my personal knowledge or from information that I have learned during my investigation, including information from financial institutions, witnesses, and others participating in the investigation.

Requested Seizure and Target Offenses

I am submitting this affidavit in support of an application for a warrant authorizing agents of the USSS involved in this investigation as described below to seize up to the value of 80,736.10 USDT (Tether) and 7.2799 BTC (Bitcoin) from the below described wallet, hereinafter the “**Target Cryptocurrency Account:**”

All remaining USDT (Tether) at Cryptocurrency Exchange Binance, not to exceed 80,736.10 USDT (TetherUS) and 7.2799 BTC (Bitcoin) held in the Binance account associated with the owner: Haider Ali.

I respectfully submit there is probable cause to believe that the funds in the **Target Cryptocurrency Account** are unlawful proceeds of violations relating to 18 U.S.C. §§1343, 1349 (wire fraud, wire fraud conspiracy) and are thereby subject to civil and criminal forfeiture pursuant to 18 U.S.C. § 981(a)(1)(C), made applicable to criminal forfeiture by 28 U.S.C. § 2461(c). The funds described herein are also thereby subject to civil and criminal seizure pursuant to 18 U.S.C. § 981(b) and 21 U.S.C. § 853(e) and (f) by 18 U.S.C. § 982(b)(1).

Background on Cryptocurrency and Binance Exchange

Based on my training, research, education, and experience, I am familiar with the following relevant terms and definitions as they relate to cryptocurrency:

Cryptocurrency: Cryptocurrency, a type of virtual currency, is a decentralized, peer-to-peer, network-based medium of value or exchange that may be used as a substitute for fiat currency to

buy goods or services or exchanged for fiat currency¹ or other cryptocurrencies. Examples of cryptocurrency are Bitcoin (BTC), Litecoin (LTC), Ethereum (ETH) and Tether (USDT). Cryptocurrency can exist digitally on the Internet, in an electronic storage device, or in cloud-based servers. Although not usually stored in any physical form, public and private keys (described below) used to transfer cryptocurrency from one person or place to another can be printed or written on a piece of paper or other tangible object. Cryptocurrency can be exchanged directly person to person, through a cryptocurrency exchange, or through other intermediaries. Generally, cryptocurrency is not issued by any government, bank, or company; it is instead generated and controlled through computer software operating on a decentralized peer-to-peer network. Most cryptocurrencies have a “blockchain,” which is a distributed public ledger, run by the decentralized network, containing an immutable and historical record of every transaction.² Cryptocurrency is not illegal in the United States.

Wallet: Cryptocurrency is stored in a virtual account called a wallet. Wallets are software programs that interface with blockchains and generate and/or store public and private keys used to send and receive cryptocurrency. A public key or address is akin to a bank account number, and a private key is akin to a PIN number or password that allows a user the ability to access and transfer value associated with the public address or key. To conduct transactions on a blockchain, an individual must use the public address (or “public key”) and the private address (or “private key”). A public address is represented as a case-sensitive string of letters and numbers, 26–36 characters long, and is somewhat analogous to a bank account number. Each public address is controlled and/or accessed through the use of a unique corresponding private key—the cryptographic equivalent of a password or PIN—needed to access the address. Only the holder of an address’s private key can authorize any transfers of cryptocurrency from that address to another cryptocurrency address.

Cryptocurrency Wallet Services: Some companies offer cryptocurrency wallet services which allow users to download a digital wallet application onto their smart phone or other digital device. A user typically accesses the wallet application by inputting a user-generated PIN code or password. Users can store, receive, and transfer cryptocurrencies via the application; however, many of these companies do not store or otherwise have access to their users’ funds or the private keys that are necessary to access users’ wallet applications. Rather, the private keys are stored on the device on which the wallet application is installed (or any digital or physical backup private key that the user creates). As a result, these companies generally cannot assist in seizing or otherwise restraining their users’ cryptocurrency. Nevertheless, law enforcement could seize cryptocurrency from the user’s wallet directly, such as by accessing the user’s smart phone, accessing the wallet application, and transferring the cryptocurrency therein to a law enforcement-controlled wallet. Alternatively, where law enforcement has obtained the recovery seed for a wallet (see above), law enforcement may be able to use the recovery seed phrase to recover or reconstitute

¹ Fiat currency is currency issued and regulated by a government, such as the U.S. dollar, euro, or Japanese yen.

² Some cryptocurrencies operate on blockchains that are not public and operate in such a way to obfuscate transactions, making it difficult to trace or attribute transactions.

the wallet on a different digital device and subsequently transfer cryptocurrencies held within the new wallet to a law enforcement-controlled wallet.

Use of Cryptocurrency in Criminal Activity: Although cryptocurrencies such as Bitcoin, Ethereum, and Tether have legitimate uses, cryptocurrency is also used by individuals and organizations for criminal purposes, such as money laundering, and is often used as payment for illegal goods and services. By maintaining multiple wallets, those who use cryptocurrency for illicit purposes can attempt to thwart law enforcement's efforts to track transactions.

BTC Value in U.S. Dollars: As of March 7, 2024, one BTC is worth approximately \$67,944, though the value of BTC is generally much more volatile than that of fiat currencies.

Exchanges: Cryptocurrency “exchangers” and “exchanges” are individuals or companies that exchange bitcoin for other currencies and cryptocurrencies, including U.S. dollars and Tether/USDT. Exchanges can be brick-and-mortar businesses or online businesses (exchanging electronically transferred money and virtual currencies). According to Department of Treasury, Financial Crimes Enforcement Network (“FinCEN”) guidance issued on March 18, 2013, virtual currency administrators and exchangers, including an individual exchanger operating as a business, are considered money services businesses.³ Such exchanges and exchangers are required to register with FinCEN and have proper state licenses (if required under applicable state law). Based on my training and experience, I know that registered money transmitters are required by law to follow Bank Secrecy Act anti-money laundering (“AML”) regulations, “Know Your Customer” (“KYC”) protocols, and other verification procedures similar to those employed by traditional financial institutions. For example, FinCEN-registered cryptocurrency exchangers often require customers who want to open or maintain accounts on their exchange to provide their name, address, phone number, and the full bank account and routing numbers that the customer links to an exchange account. As a result, there is significant market demand for illicit cryptocurrency-for-fiat currency exchangers, who lack AML or KYC protocols and often also advertise their ability to offer customers stealth and anonymity. These illicit exchangers routinely exchange fiat currency for cryptocurrencies by meeting customers in person or by shipping cash through the mail. Due to the illicit nature of these transactions and their customers' desire for anonymity, such exchangers are frequently able to charge a higher exchange fee, often as high as 9–10% (in contrast to registered and BSA-compliant exchangers, who may charge fees as low as 1–2%).

Exchange Transactions: Exchangers and users of cryptocurrencies store and transact their cryptocurrency in a number of ways, as wallet software can be housed in a variety of forms, including on a tangible, external device (“hardware wallet”), downloaded on a PC or laptop (“desktop wallet”), with an Internet-based cloud storage provider (“online wallet”), as a mobile application on a smartphone or tablet (“mobile wallet”), printed public and private keys (“paper

³ See “Application of FinCEN’s Regulations to Person Administering, Exchanging, or Using Virtual Currencies,” available at <https://www.fincen.gov/resources/statutes-regulations/guidance/application-fincens-regulations-persons-administering>.

wallet”), and as an online account associated with a cryptocurrency exchange. Because these desktop, mobile, and online wallets are electronic in nature, they are located on mobile devices (e.g., smart phones or tablets) or at websites that users can access via a computer, smart phone, or any device that can search the Internet. Moreover, hardware wallets are located on some type of external or removable media device, such as a USB thumb drive or other commercially available device designed to store cryptocurrency (e.g. Trezor, Keepkey, or Nano Ledger). In addition, paper wallets contain an address and a QR code⁴ with the public and private key embedded in the code. Paper wallet keys are not stored digitally. Wallets can also be backed up into, for example, paper printouts, USB drives, or CDs, and accessed through a “recovery seed” (random words strung together in a phrase) or a complex password. Additional security safeguards for cryptocurrency wallets can include two-factor authorization (such as a password and a phrase). I also know that individuals possessing cryptocurrencies often have safeguards in place to ensure that their cryptocurrencies become further secured in the event that their assets become potentially vulnerable to seizure and/or unauthorized transfer.

Binance: Binance is a global cryptocurrency spot and derivatives exchange. They report to be the largest cryptocurrency in terms of daily volume. Binance serves customers from around the world but does not do business in the United States. There is no official company headquarters, but the organization was founded in 2017 in Shanghai, China. Binance owns several companies including TRUST wallet application used to store and manage cryptocurrency wallets.

Cryptocurrency ATM: Cryptocurrency ATM (CATM) allows consumers to purchase and sell Bitcoin and other cryptocurrencies. The device resembles a conventional ATM and operates in a similar fashion. CATMs are generally placed in commercial businesses such as gas stations, liquor stores, and retail outlets. After providing the CATM with identification, such as a phone number, the customer enters the address of the digital wallet that will receive the Bitcoin purchased, usually using a QR code. Transactions are usually completed by feeding cash into the machine and the CATM company sends a specified amount of the chosen cryptocurrency. Examples of CATMs include Bitcoin Depot, Athena Bitcoin, and Coinhub ATMs.

Bitcoin Change Wallet: In Bitcoin transactions, a change wallet is the identified wallet that is used to store the excess bitcoins not sent to the recipient of the transaction. When the amount of Bitcoin sent to the recipient is less than the total amount of Bitcoin contained in the sender’s wallet, the excess is sent to a change wallet controlled by the sender. Bitcoin transactions require that all coins in the sender’s wallet are sent for each transaction. The change wallet, often automatically controlled by the wallet software, is typically new and does not contain any additional cryptocurrency. Commercially available cryptocurrency tracing tools have the ability to identify change wallets based on transaction patterns and AI algorithms.

⁴ A QR code is a matrix barcode that is a machine-readable optical label.

Probable Cause

Use of Target Cryptocurrency Wallet in Wire Fraud

For the reasons described below, I submit there is probable cause to believe target(s) HAIDER ALI and IRFAN SIDDIQUE (as described below) operate the **Target Cryptocurrency Account** to perpetuate the scheme described herein.

Subjects

South Carolina Law Enforcement Division (SLED) Special Agents assigned to the US Secret Service Cyber Fraud Task Force were contacted by detectives with the West Columbia Police Department (WCPD) on January 25, 2024, in reference to a financial fraud (WCPD Report# 2402880). Agents determined that the individual (Victim 1) was the victim of a fraud scheme and had sent Bitcoin under a scheme to defraud using a cryptocurrency ATM. Agents traced the cryptocurrency transaction and determined that the funds were sent to an identified Bitcoin cryptocurrency wallet with Binance (**Target Cryptocurrency Account**). On January 30, 2024, agents submitted a memo requesting that Binance place a temporary hold on the funds and provide “KYC” documentation regarding the owner of the **Target Cryptocurrency Account**. Binance responded by placing a temporary freeze on the account based on the information and provided a spreadsheet with KYC information. The records identified the owner as HAIDER ALI with the associated email address “mi5siddique@gmail.com” and phone number “+919007696476”. Binance provided the government ID used to establish the account showing the name HAIDER ALI.

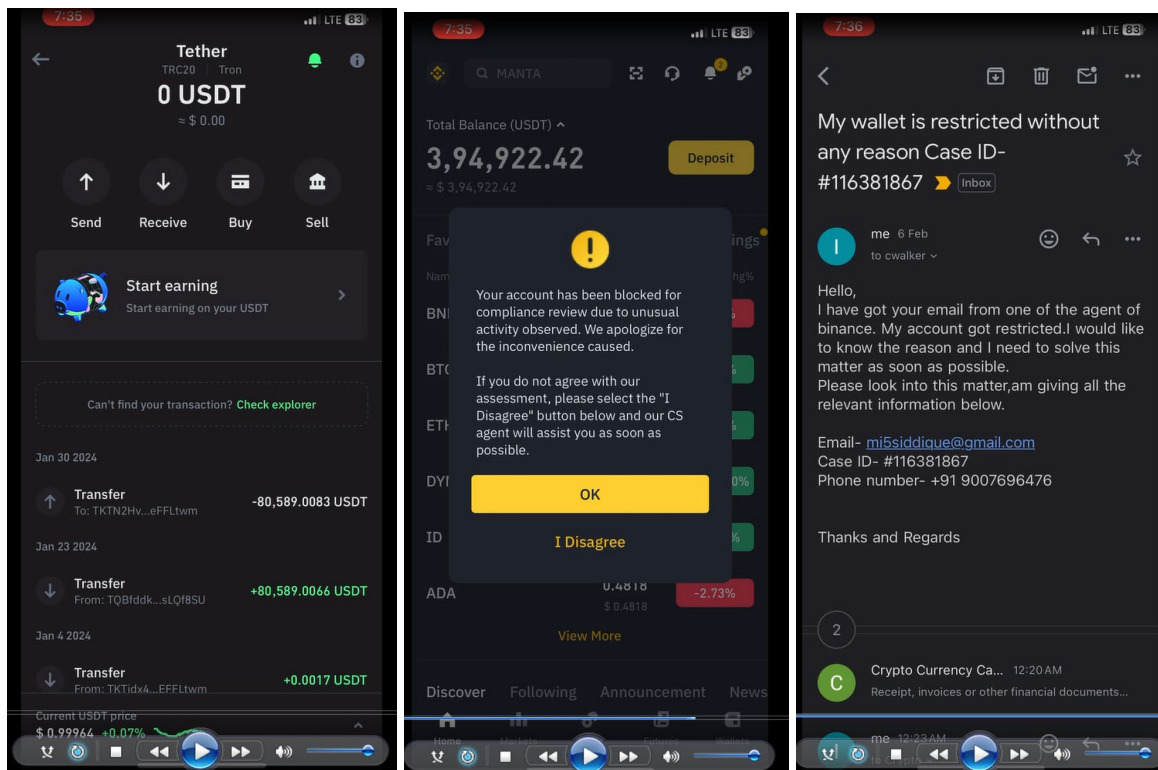


Image of ID provided by Binance.

The KYC documents contained the transaction history associated with the Binance account as well as the current balance of 80,736.10 USDT (TetherUS) and 7.2799 BTC (Bitcoin). On February 6, 2024, I received an email from “Irfan Siddique <mi5siddique@gmail.com>”, matching the email associated with the **Target Cryptocurrency Account** inquiring about the reason for the Binance account freeze. The sender (**SIDDIQUE**) provided the Binance case number, email, and phone number associated with the **Target Cryptocurrency Account** as a means of contact. I replied to the email stating the freeze was due to suspected fraud and asked for information regarding the transactions and any legitimate documentation that could be provided regarding the transactions.

SIDDIQUE sent several emails requesting clarification on the type of documents. I responded with examples of documents that would prove a legitimate business purpose for the funds. On February 7, 2024, I received an email from “mi5siddique@gmail.com” that contained an attached video that is consistent with a screen recording taken from an Apple iOS device. The video depicts an individual opening the “TRUST Wallet” and Binance Mobile apps. When attempting to navigate the Binance app, the video shows a popup stating that “the account has been

blocked for compliance review”. The video ends with the user navigating to the “Gmail” email application and showing the email correspondence between myself and **SIDDIQUE**.



Screenshots taken from the video sent to the affiant on 2/7/24.

SIDDIQUE stated in the email the video was sent to prove ownership over the frozen Binance account. **SIDDIQUE** stated that the funds were bought from “local P2P,” (peer-to-peer) and the transactions were related to cryptocurrency trading. I exchanged additional emails with **SIDDIQUE**, but he did not provide any documentation pertaining to the trades. When asked as to the reason why the transaction contained funds originating from Cryptocurrency ATMs, **SIDDIQUE** replied that *“This is really a baseless point that you are saying, I have never done or received any funds from any crypto currency ATMs or neither from any unknown person. I just use this platform for my trading purpose and saving for crypto currency.”*

On March 5, 2024, at approximately 1900 EST, I received a call to my work issued cell phone from “929-443-4855”. After answering the call, I set up my laptop and recorded the conversation. The following information is saved as a recording and is a summary of portions of the call with direct quotes noted by quotation marks. The caller had a firm grasp of the English language and communicated effectively over the phone.

The caller identified themselves as **IRFAN SIDDIQUE** of 28 Bright St, Kolkata, 70019 W Bengal India. **SIDDIQUE** stated that the purpose of the **Target Cryptocurrency Account** was for cryptocurrency trading and had been used for this purpose for several years, and he works on behalf of other clients including friends and relatives. **SIDDIQUE** stated he does not have any web site or marketing regarding the business. **SIDDIQUE** stated that he purchased the USDT from another individual in a physical market facilitated through online chat applications. **SIDDIQUE** indicated that he pays for cryptocurrency using physical currency and then is sent the agreed upon amount of cryptocurrency. **SIDDIQUE** would not provide detailed information regarding the individuals from whom the cryptocurrency was purchased. When asked about specific transactions, **SIDDIQUE** stated he would need additional time to provide documentation relating to the transaction. When asked about the reason for buying the funds from an individual and not a major exchange, **SIDDIQUE** stated that the Indian government places a 30% tax on the transaction.

SIDDIQUE said several times during the conversation that he did not know where the funds originated and stated that he had no way of knowing if cryptocurrencies were stolen. When asked if cryptocurrency trading was occurring in an underground market, **SIDDIQUE** stated *“Underground black market, you can say black market. I mean the thing is fine, [sic] ... it’s going through contact to contact.”*

During the conversation, I provided numerous examples of documents that would show legitimate business transactions related to the Binance account. **SIDDIQUE** stated that he would check with the individuals he bought the cryptocurrency from. **SIDDIQUE** also stated that the BTC wallet “**bc1qlnvrqp7ms45e9s0zmze8r25su88p6ql898yv47**” (“**SIDDIQUE** Controlled TRUST Wallet”) was under his control and managed using the TRUST wallet cryptocurrency application. This wallet was also seen in subsequent conversations where screenshots of a conversation between **SIDDIQUE** and a purported seller were emailed to me. When asked directly if they conducted any form of scamming, **SIDDIQUE** emphatically stated he did not, but he knew cryptocurrencies are sometimes used in scams. **SIDDIQUE** stated that he did not have any employees connected with the transfers and became defensive when asked about the location of his office and the sellers involved in the transactions.

The following conversation took place when **SIDDIQUE** was asked about **HAIDER ALI** and why his information was listed as the owner of the account.

SA Walker: “Can can you tell me who Haider Ali is?” *[Pause]*

SA Walker: “Are you there?”

SIDDIQUE: “Yes I can hear you.”

[Several exchanges back and forth saying and spelling “Haider Ali”]

SA Walker: “Who is that?”

SIDDIQUE: “Haider Ali is my friend.”

SA Walker: “So why is his info in the Binance account information?”

SIDDIQUE: “His phone is being verified from him”

***SA Walker:** “OK, but when we first started talking you said this was your account?”*

***SIDDIQUE:** [Unintelligible]*

***SA Walker:** “[SIC] But you said your name was Irfan Siddique.”*

***SIDDIQUE:** “Haider ALI is my friend, He is my brother, and anything you want, you need regarding this I can provide no problem.”*

***SA Walker:** “OK, But but when we started talking, you said this was your account.”*

***SIDDIQUE:** “Yes, obviously I am handling this account. It belongs to me only.”*

***SA Walker:** “OK, Is your name Haider ALI? Are you there, I can’t hear you.”*

***SIDDIQUE:** “Yes, Haider Ali is my friend and he's the one who created this account.”*

SIDDIQUE was asked several follow up questions regarding his identity and his relationship with **ALI**.

***SIDDIQUE:** “I have already told you my name is Irfan SIDDIQUE and this account is being verified by one of my friend and my brother is we, we we we work together”*

***SA Walker:** “OK, So he works at the business with you?”*

***SIDDIQUE:** “Yes”*

SIDDIQUE stated that he had several other side jobs and cryptocurrency trading was not his full-time job. He would not provide the contact information for **HAIDER ALI**.

SA Walker: “At this point, look at it from my side, how do I know that you haven’t stole Mr. Ali’s account. You know what I’m saying?”

SIDDIQUE: “Uh, I since [unintelligible] updated this account, Right? And it’s been like, two, three, See one more thing. If I have stolen his account, If I have stolen his account, anything like that. So he he he would have contacted to this thing. Binance or whatever. Who’s contacting? I’m contacting. Yeah, he only created his account like, but I’m the one who is, like, dealing. And all of this, whatever purchasing, buying or whatever this thing. So this nothing like that, Sir. I don’t like, go on that train, like this is stolen account. The first very first time I used to like log in my account in this phone.”

SIDDIQUE stated that he had issues logging into the Binance application and that he had to use another phone to log into the application.

SA Walker: “So you’re telling me that Mr. Ali is also able to log into the account?”

SIDDIQUE: “No, No, No. I’m handling this account and this belongs to, my responsibility. This account is verified by him.”

I continued to question him regarding the operations of the **Target Cryptocurrency Account**.

SA Walker: “I would very much like to talk to him (**ALI**) because clearly this, you know, these transactions, he’s to be honest, he’s actually the one that that I really need to be talking to. Because these all these transactions are under his name.

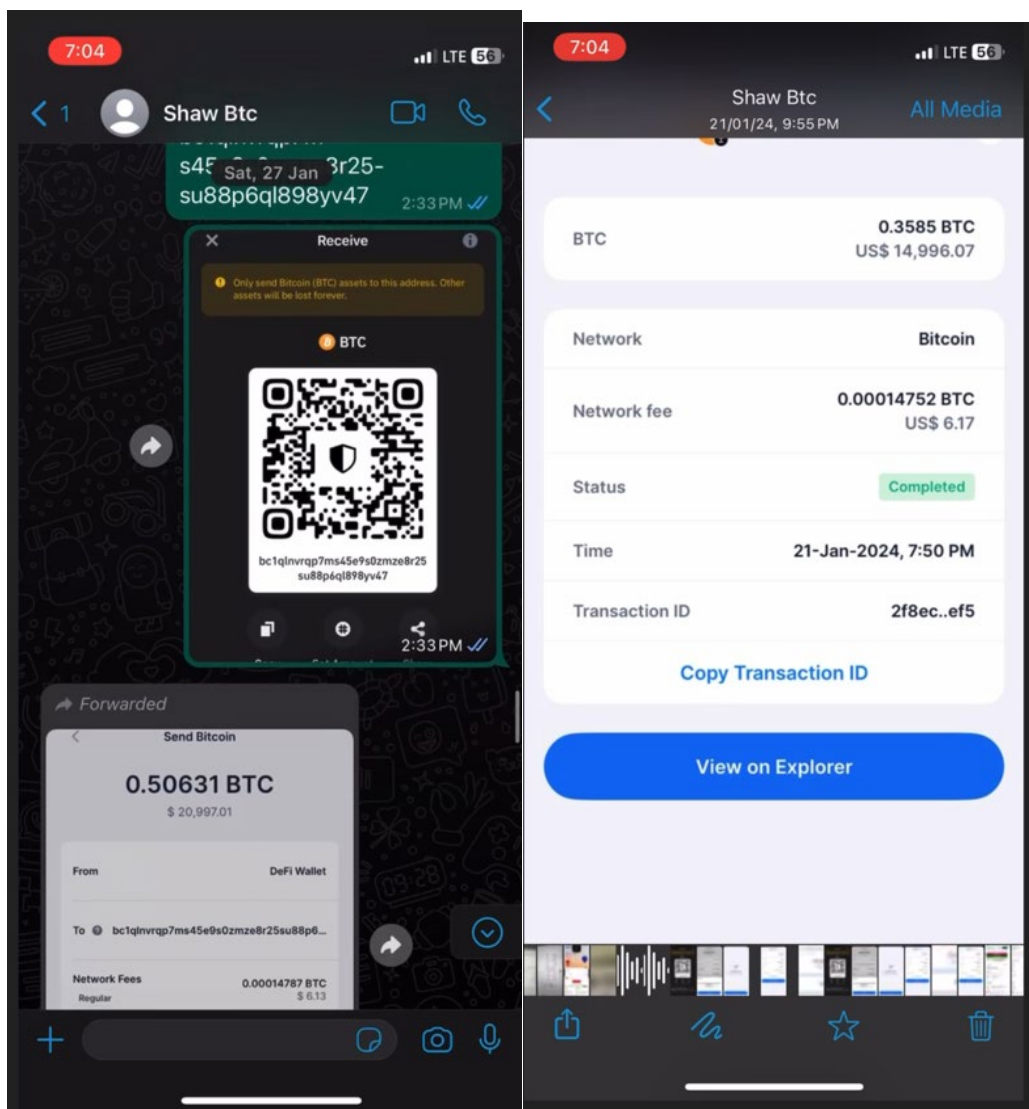
SIDDIQUE: “To be honest, this device is being used by me from day one and whatever purchase and whatever, then whatever this thing is all done by my thing.”

SIDDIQUE stated that I could talk to **ALI**, but he is not fluent in English. The phone call was disconnected after several attempts to confirm who had control of the wallet. I called the number back and **SIDDIQUE** answered. The conversation continued and **SIDDIQUE** continued to give evasive answers when asked about his identity and declined to provide a copy of his ID upon request. When challenged about **ALI**'s involvement in the cryptocurrency trading, **SIDDIQUE** stated that **ALI** sat beside him during trading and was aware of the trading activity.

SIDDIQUE was asked repeatedly about if he knew the funds were stolen. **SIDDIQUE** stated he would never trade in funds he knew were stolen. The conversation continued and many of the topics discussed centered around **SIDDIQUE** requesting that the account be unfrozen. The conversation subsequently ended with a request for documentation from **SIDDIQUE** who stated he would provide information regarding the transactions.

I received several more emails from **SIDDIQUE** after the call. One email contained a video consistent with a screen recording from an Apple iOS device that depicts a text message conversation in the application WhatsApp. The recipient is shown as "Shaw Btc". On March 27, 2024, I received a call from 916-655-2871. They identified themselves as Irfan **SIDDIQUE**. During the conversation, I asked **SIDDIQUE** to explain the messages in the conversation with "Shaw Btc". **SIDDIQUE** explained that this was a conversation with an individual known to him as "Shaw" and a seller of cryptocurrency. The text message depicts two transactions that took place on January 21 and 27. **SIDDIQUE** explained that cryptocurrency was sent to "bc1qlnvrqp7ms45e9s0zmze8r25su88p6ql898yv47" identified as "SIDDIQUE Controlled TRUST Wallet" from "Shaw". The transaction shown in the video sent on January 27 is associated with the funds from Victim 1 and Victim 2 based on the times and transaction IDs shown in the text message conversation.

SIDDIQUE denied that “Shaw” was a scammer and stated that he was a share market trader and crypto dealer. **SIDDIQUE** had knowledge “Shaw” was engaged in other business but did not know exactly what they did. The conversation continued and **SIDDIQUE** was again asked to provide additional information regarding the transactions. **SIDDIQUE** later provided the WhatsApp number for “Shaw Btc” (+917980668718).



Screenshots taken from the video sent to the affiant on 3/13/24 showing details consistent with the cryptocurrency associated with the funds sent from Victim 1 and Victim 2.

Victim 1

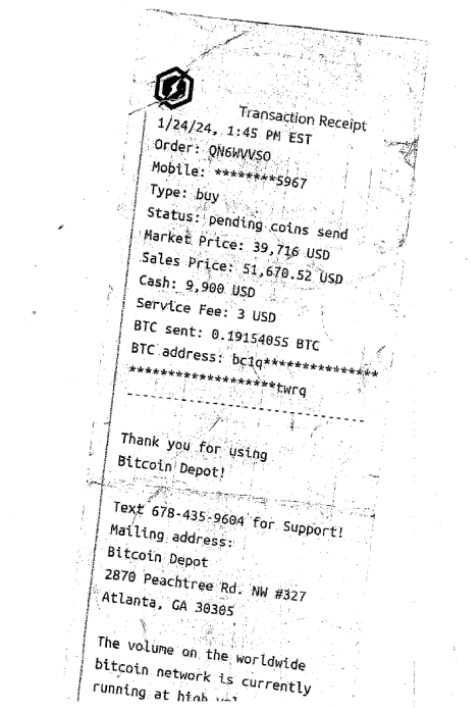
On January 25, 2024, detectives with the West Columbia Police Department (WCPD) contacted the South Carolina Law Enforcement Division (SLED) Special Agents assigned to the US Secret Service Cyber Fraud Task Force in reference to a financial fraud (WCPD Report# 2402880). Agents met with the victim and conducted an interview and electronic forensic exam with the written consent of the victim.

On the morning of January 24, 2024, M. L. (Victim 1) of West Columbia, SC, received an email from “froncesgoodzoi117@gmail.com” purporting to be a Paypal receipt for Norton Anti-virus software for approximately \$259. Victim 1 called the number on the purported Paypal receipt to dispute the charge and was connected with individuals who stated they were employees of Paypal. Victim 1 was directed to submit information to complete the refund process using a Google form. Victim 1 allowed the individuals access to his/her computer and online banking accounts. While viewing Victim 1’s Truist bank account, the individuals stated that during the refund process, a typo resulted in \$50,000 being deposited into Victim 1’s account. The subject manipulated the HTML of Victim 1’s Truist Account causing the appearance of the balance of Victim 1’s account to change without accessing the actual funds. Victim 1 was directed to withdraw \$10,000 in USD from his/her Truist bank account.

After withdrawing the funds, Victim 1 was directed to a Bitcoin Depot ATM located at 1600 Holland St, West Columbia, SC (Simba Mini Mart). Victim 1 was provided with a cryptocurrency address in the form of a QR code and sent 0.19154055 BTC (\$9,900) using the Bitcoin Depot ATM. After the bitcoin transaction was completed, Victim 1 was directed to

withdraw \$30,000 in USD for the remainder of the refund payment. The victim traveled to their bank and withdrew \$30,000 in \$100 and \$50 bills. An unidentified individual arrived at Victim 1's home and retrieved an envelope containing \$30,000.

Based on the partial address provided on the receipt and tools available to law enforcement, I determined the funds were transferred to the BTC wallet "bc1qaurlnpejmcu3euqz3xsn2e9jjltrc2v8ptwrq".



*Receipt of transaction provided by **Victim 1**.*

During the investigation, I traced the funds sent by Victim 1 using commercially available cryptocurrency tracing software. On January 27, 2024, the 0.19154055 BTC attributed to Victim 1, as well as four other BTC wallets with a combined value of 0.696052 BTC were transferred. (Attachment 1). A wallet included in this transaction was later identified as being associated with N.J.T. (Victim 2). All wallets included in the transfer contained funds that originated from Cryptocurrency ATMs. The transaction resulted in 0.50631 BTC being sent to BTC wallet

“bc1qlnvrqp7ms45e9s0zmze8r25su88p6ql898yv47” identified as SIDDIQUE Controlled TRUST Wallet. The remainder of the transaction was sent to an unidentified Bitcoin change address. On January 30, 2024, 0.872169 BTC was transferred from the SIDDIQUE Controlled TRUST Wallet to a wallet associated with the **Target Cryptocurrency Account**. (Attachment 1). Victim 1 reported that the total monetary loss resulting from the fraud was approximately \$50,900.

Victim 2

During the investigation, I used law enforcement databases to identify additional victims associated with the identified cryptocurrency transactions. I identified N. J. T. (Victim 2) of Rapid City, South Dakota, as being an additional victim in the fraud scheme. On January 26, 2024, Victim 2 received an email from Paypal stating their money had been compromised and he/she needed to call the fraud department using the number provided in the email. The individuals who answered the call identified themselves as Paypal employees and told the victim that his/her identity had been stolen and additional measures would have to be taken to secure it.

Victim 2 was instructed to buy gift cards at local stores to start the refund process and subsequently sent \$2,000 worth of gift cards of various services to the subjects purporting to be Paypal support. Victim 2 was also directed to download an app that would allow remote access to their phone. The subjects on the phone then directed Victim 2 to withdraw \$15,000 from an account he/she controlled and send the money using a Cryptocurrency ATM. Victim 2 placed \$14,900 into the Bitcoin Depot cryptocurrency ATM located at 1846 Eglin St, Rapid City, South Dakota 57701 and purchased 0.27361 BTC. Victim 2 filed a report (SCR24-100614) with the Pennington County Sheriff's Office on 1/31/24. A search warrant submitted to Bitcoin Depot identified Victim 2 sent

0.27361 BTC to BTC wallet “bc1qjrxs62hwzag55xcu88qsehjhktnp5q6m7m6fy”. (Attachment 1).

On January 27, 2024, the 0.27361 BTC associated with the payment from Victim 2 was transferred, along with the funds associated with Victim 1, to the SIDDIQUE Controlled TRUST Wallet. (Attachment 1). On January 30, 2024, 0.872169 BTC was transferred from the SIDDIQUE Controlled TRUST Wallet to a wallet associated with the **Target Cryptocurrency Account**. Victim 2 reported that the total monetary loss resulting from the fraud was approximately \$16,900.00.

Victim 3

During the investigation, I used law enforcement databases to identify additional victims associated with the identified cryptocurrency transactions. I identified M. T. S. (Victim 3) of Vale, North Carolina, as an additional victim involved in the fraud scheme. The victim reported (LCSO# 2023-06554) the incident to the Lincoln County Sheriff’s Office on October 30, 2023.

Victim 3 reported that on the morning of October 30, 2023, he/she received an alert on his/her computer to renew the anti-virus software for \$380.00. During the supposed refund process, Victim 3 reported that extra zeros were added to the refund amount resulting in the refund amount being \$38,000. Victim 3 was then directed to contact a number for customer support. Victim 3 was directed by the purported customer support representative that a wire for \$38,000 was sent to their bank account and additional steps would have to be taken to recover the funds. Victim 3 was directed to withdraw the funds from his/her bank account and return the money to the individuals on the phone. Victim 3 withdrew \$12,500 in cash from his/her bank account and traveled to a gas station where he/she placed the funds into a cryptocurrency ATM. The victim attempted to send

approximately \$25,000 through overnight mail, but the shipment was stopped, and the funds were recovered.

Using law enforcement databases, I was able to determine the transaction occurred using a Bitcoin Depot ATM. Using commercially available cryptocurrency tracing software, I determined that 0.279861 BTC was sent to BTC wallet “**bc1qeyxyrdvwy5yf88qlzznr9rx5lj9uzsh2dlxlut**” by Victim 3. On November 2, 2023, the 0.279861 BTC was sent along with two other wallets to SIDDIQUE Controlled TRUST Wallet. (Attachment 2). The funds were transferred to BTC Wallet “**bc1qxkt09zc5zpqacla8m7ae89m806ph5y4dxhm4hs**” on the same day. On December 2, 2023, the **Target Cryptocurrency Account** received 2.05004 BTC from “**bc1qxkt09zc5zpqacla8m7ae89m806ph5y4dxhm4hs**”. (Attachment 2).

Victim 4

During the investigation, I used law enforcement databases to identify additional victims associated with the identified cryptocurrency transactions. I identified D.T. (Victim 4) of Upper Arlington, Ohio, as an additional victim involved in the fraud scheme. Several attempts to call the victim were unsuccessful. I made contact with Victim 4 over the phone April 13, 2024, at an assisted living facility with the help of administrators and the facilities social worker. Victim 4 stated they were originally contacted in or around 2021 by email stating they were entitled to federal funds. Victim 4 sent money through Cryptocurrency ATMs as well as the mail. Victim 4 estimated that since the start of the scam they had sent approximately \$20,000 through the mail and \$80,000 through Bitcoin using cryptocurrency ATMs in several states. The transaction identified during the investigation was one of the last transactions Victim 4 conducted before breaking off contact with the fraud subjects. Victim 4 had not filed any reports with law

enforcement prior to being contacted by the affiant. On September 6, 2023, Victim 4 sent 0.13434 BTC through a Bitcoin Depot ATM to BTC address “**bc1qktl3pjtm45w39pdapht79vx6v8ak0az7sy3pwe**”. (Attachment 3). On November 8, 2023, BTC wallet “**bc1qktl3pjtm45w39pdapht79vx6v8ak0az7sy3pwe**” sent 1.09677 BTC to SIDDIQUE Controlled TRUST Wallet. (Attachment 3).

Victim 5

During the investigation, I used law enforcement databases to identify additional victims associated with the identified cryptocurrency transactions. I identified W.M. (Victim 5) of Beltsville, Maryland, as an additional victim involved in the fraud scheme. On February 3, 2024, Victim 5 submitted a complaint to the FBI (I2402031317298223) stating he/she was the victim of a fraud involving Bitcoin. The description of the complaint per Victim 5 is as follows:

“Responded to an email about a charge that I questioned. Resulted in the scammers making it look as though they deposited \$10,000 in my account (I later realized they just transferred the money from my savings account to my checking account. I was instructed to send the money back to them through a Bitcoin atm.”

Victim 5 indicated that the fraud transaction occurred using Athena Bitcoin ATM. Using this information, I determined that on February 2, 2024, Victim 5 sent 0.16509 BTC from an Athena Bitcoin ATM to BTC wallet “**bc1q0vywm02r8lrkxhj9tzzawp5g9zu252egg9p0**”. On February 3, 2024, 0.164479 BTC was sent from “**bc1q0vywm02r8lrkxhj9tzzawp5g9zu252egg9p0**” to SIDDIQUE Controlled TRUST Wallet. (Attachment 4).

Cryptocurrency Transactions

During the investigation, agents requested that Binance place a temporary hold on the funds and provide “KYC” documentation regarding the owner of the **Target Cryptocurrency Account**. The KYC documentation provided included transaction records associated with the **Target Cryptocurrency Account**. The **Target Cryptocurrency Account** was created on April 28, 2021, with the name HAIDER ALI and email “mi5siddique@gmail.com”. The account balance as of January 31, 2024, was 80,736.10 USDT (TetherUS) and 7.2799 BTC (Bitcoin). Records show the account has received a total of eleven BTC Deposits. The **Target Cryptocurrency Account** consists of one BTC wallet, “12jhQm39LX44NihVRWwF4FgN9LEDK6h2Vr” with a total inflow of 6.583894 BTC. Funds associated with Victims 1-4 were received by BTC wallet “12jhQm39LX44NihVRWwF4FgN9LEDK6h2Vr”.

All victims of fraud identified during this investigation were above the age of 60 when the fraud occurred. Based on my training and experience, the **Target Cryptocurrency Account** is being used to transact in and launder funds from scams targeting elderly individuals. The investigation also determined four additional possible identified victims. These potential victims ranged in age from 72 to 78 at the time of the possible fraud transaction. All possible victims used a cryptocurrency ATM to send cryptocurrency that was traced to SIDDIQUE Controlled TRUST Wallet during the timeframe of identified fraud.

Based on the investigation as well as the recorded admissions made by **SIDDIQUE**, it is the affiant’s belief that the **Target Cryptocurrency Account** is being used to receive funds directly tied to a scheme or artifice to defraud U.S. based victims of elder fraud. By their own admission during a conversation with the affiant, **SIDDIQUE** stated he is operating a “black market” business

with the express purpose of circumventing tax law in his country of residence. **SIDDIQUE** also clearly stated that he provided false information when registering the account in the name of Haider ALI. Based on my training and experience, I believe that **SIDDIQUE** registered the account in the name of ALI to commit fraud while concealing his identity. It is the affiant's belief that all funds associated with the account should be seized pursuant to this investigation.

Conclusion and Authority

Though the Target Cryptocurrency Wallet is believed to be located outside the District of South Carolina, 18 U.S.C. § 981(b)(3), as amended by the Civil Asset Forfeiture Act of 2000 ("CAFRA"), Pub. L. No. 106-185, 114 Stat. 202 (2000), provides jurisdiction for the issuance of seizure warrants for property located in other districts. That is, the issuance of the seizure warrant in this district is appropriate under 18 U.S.C. § 981(b)(3), and 28 U.S.C. § 1355(b)(1) because, notwithstanding the provisions of Rule 41(a) of the Federal Rules of Criminal Procedure, a seizure warrant may be issued by a judicial officer in any district in which a forfeiture action against the property may be filed.

Notwithstanding the provisions of Rule 41(a) of the Federal Rules of Criminal Procedure, a seizure warrant may be issued pursuant to this subsection by a judicial officer in any district in which a forfeiture action against the property may be filed under section 1335(b) or Title 28 and may be executed in any district in which the property is found.

Thus, the issuance of the seizure warrant in this district is appropriate under the above statute, as this is the district "in which ... the acts or omissions giving rise to the forfeiture occurred," and based on my training and experience, this is a continuance of an "elder fraud scam" that began with the original victim who is based in West Columbia, South Carolina. Further, "venue for the forfeiture action . . . is specifically provided for in section 1395." 28 U.S.C. § 1355(b)(1)(A)

and (B). Section 1395 provides “for the recovery of a . . . forfeiture . . . in the district where it accrues.”

I submit there is probable cause to believe the funds in the **Target Cryptocurrency Wallet** are proceeds traceable to violations of 18 U.S.C. §§ 1343, 1349 (wire fraud, conspiracy to commit wire fraud) and subject to civil and criminal forfeiture to the United States pursuant to 18 U.S.C. § 981(a)(1)(C) made applicable to criminal forfeiture by 28 U.S.C. § 2461(c) and are thereby also subject to seizure pursuant to 18 U.S.C. § 981(b) and 21 U.S.C. § 853(e) and (f) by 18 U.S.C. § 982(b)(1).

Further, a restraining order would not be adequate to preserve the property for forfeiture as the funds in the cryptocurrency account can be easily moved, transferred, or dissipated. Therefore, I respectfully request the issuance of a seizure warrant that will authorize the seizure of funds contained in the cryptocurrency account described herein.

This affidavit has been reviewed by Assistant U.S. Attorneys Carrie Fisher Sherard and Lothrop Morris.

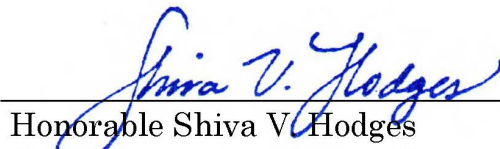
I swear, under penalty of perjury, that the foregoing is true and correct to the best of my knowledge.

Sworn pursuant to Fed. R. Crim. P. 4.1(b)(2)(A) this ___ day of May, 2024



Clinton Walker
Special Agent
United States Secret Service Cyber Fraud Task Force

This affidavit was sworn to by the affiant, who attested to its contents pursuant to Fed. R. Crim. P. 4.1(b)(2)(A) by telephone after a document was transmitted by email pursuant to Fed. R. Crim. P. 4.1.



Honorable Shiva V. Hodges
United States Magistrate Judge

